system in either Schenck or Okamoto. Accordingly, the Applicants respectfully request the Examiner to reconsider Claims 31-40 with the amendments.

Claim 41, supported in FIG. 3, recites "a client machine executing a document securing module that operates in a path through which the electronic data is caused to pass when selected, the document securing module determining security nature of the electronic data, ... wherein the client machine and a user thereof are caused by the document securing module to be authenticated with the access control server when the security nature indicates that the electronic data is secured...". In contrast, Schenck sends demanded data in encryption to a user who has, for example, made a payment and is therefore authorized to access the data. There is no any teaching in Schenck about a document securing module (in a client machine) that causes both the client machine as well as the user to be authenticated when the document securing module determines that the data being accessed is secured. Accordingly, the Applicants respectfully request the Examiner to reconsider Claim 41.

Claim 47 recites that "...an access control server coupled to the client machine over a network and receiving a part of the electronic data including the encrypted security information from the client machine, the encrypted security information being decrypted with a user key associated with a user attempting to access the electronic data after both the user and the client machine are authenticated;" (*emphasis added*) In other words, a part of the secured file including the encrypted security information is transported to a server wherein the encrypted security information is decrypted with a user key in the server. Schenck encrypts data in a server (distributor) and sends off the encrypted data to user, and neither teaches nor suggests that the security information is decrypted in a server or the distributor. Accordingly, the Applicants submit that Claim 47 shall be allowable over Schenck and respectfully request the Examiner to reconsider Claims 47.

Claims 48-62 and 64-80, and 82-88 are rejected with similar reasons in the Office Action. The Applicants wish to apply the reasons presented above to support Claims 48-62, 64-80, and 82-88. Accordingly, Claims 48-62, 64-80, and 82-88 are believed equally patentable over the cited references, viewed alone or in combination.

(*emphasis added*)

According to Schenck, for data to be encrypted in a distributor 102 for distribution to a user, a distributor 102 must possess a public key. As described above, the server in the present invention is to provide access control management and not to encrypt the data. As such, *a client machine is used to encrypt data and decrypt encrypted data*, and therefore, maintains a private key and a public key for an authorized user. Claim 20 further explicitly recites "encrypting the security information with the public key in the client machine when the electronic data is to be written into a store; and decrypting the security information with the private key in the client machine when the electronic data is to be accessed by an application." (*emphasis added*) Evidently, the combined features are neither taught nor suggested in Schenck or Okamoto, viewed alone or in combination. In fact, Schenck or Okamoto teaches away from the features of Claim 20 as one machine is required to possess a key to encrypt data and another machine is required to possess a counterpart key to decrypt the received encrypted data. Accordingly, the Applicants submit Claim 20 and dependent claims 21-30 shall be allowable over Schenck or Ozog, viewed alone or in combination. Reconsideration of Claims 20-30 is respectfully requested.

Claim 31, in particular, recites:

receiving a request to access the electronic data in a store;
determining security nature of the electronic data by intercepting the electronic data moving from the store through an operating system layer to an application for the data;
...

(*emphasis added*)

As shown in FIG. 3, data is stored in a store 308. When the data is accessed by an application 306, the data moves through the OS 304 in which the data is intercepted by a document securing module 302 to perform the determination of the security nature of the data and decryption of the encrypted data if the data is encrypted. Subsequently, the application receives the data in clear form. Such combined features recited in Claim 31 are not at all taught or suggested in Schenck or Okamoto, viewed alone or in combination. *In fact, there is no any teaching about interception of data in an operating*

other words, Schenck provides an on-demand data method. A server or the distributor 102 is configured to encrypt demanded data and transmit the demanded data in encryption to a demander (i.e., a user), namely, the encrypted data must be from the distributor 102.

In contrast, the twice-amended **Claim 1** recites:

> establishing a secured link between a server providing the access control management and a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is not from the server but secured in a format including security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion;
>
> ...

(*emphasis added*)

Contrary to Schenck, Claim 1 explicitly recites that *a server provides the access control management but not the encrypted data* (i.e., the *encrypted data* is not from this server). As described in FIG. 1A and 1B and corresponding description thereof, the server 104 or 106 is configured to provide the access control management and not used to encrypt a data file therefore *the secured electronic data is not from the server*.

Similar to Schenck, Okamoto also teaches a distribution server for distributing digital data (*see* 301 of FIG. 3 and [0055] in Okamoto). Neither one of the two cited references has taught or suggested the features recited in Claim 1. In fact, both have taught away from the invention recited in Claim 1. Accordingly, the Applicants submit Claim 1 and dependent claims 2-15 and 17-30 shall be allowable over Schenck or Okamoto, viewed alone or in combination. Reconsideration of Claim 1-15 and 17-30 is respectfully requested.

Claim 20 recites more explicitly that data is not encrypted in a server by:

> maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when or where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme; ...